EXHIBIT D

K&L GATES

March 19, 2020

George C. Summerfield
george.summerfield@klgates.com
(312) 807-4376

SUBJECT TO FRE 408
VIA ELECTRONIC MAIL

Brian Ankenbrandt
Senior Legal Counsel - IP Transactions
Apple, Inc.
One Apple Park Way
Cupertino, California 95014

Re: Charter Pacific Corporation Ltd. Patent Portfolio

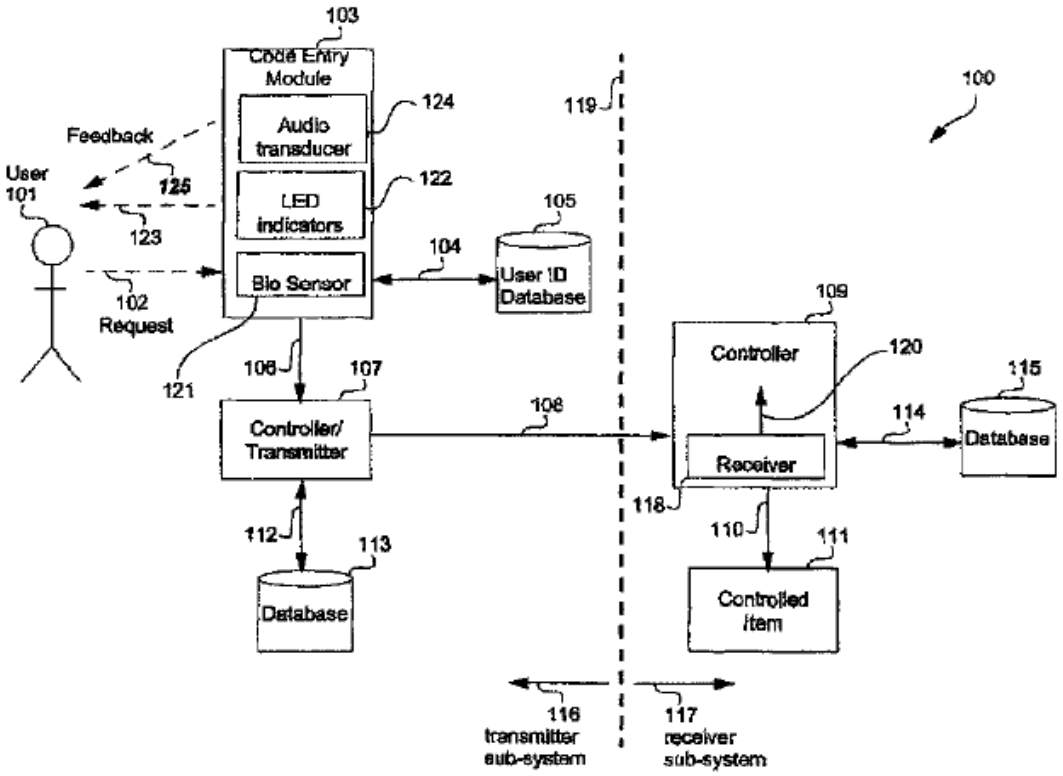
Dear Mr. Ankenbrandt:

We represent Charter Pacific Corporation Ltd/ ("Charter") in connection with its licensing and enforcement of its patent portfolio generally directed to electronic access security measures. That portfolio includes U.S. Patent No. 9,665,705 ("the '705 Patent"). I understand that the '705 Patent, its application, and its European counterpart have been the subject of previous correspondence between Charter and Apple, Inc. ("Apple"). As you alluded to in your March 5, 2020, the '705 Patent issued from U.S. Patent App. No. 15/000818, which claims priority of August 13, 2004. Although the '705 Patent has been the subject of prior correspondence, I attach a copy thereof for your convenience.

It appears from the prior correspondence that there is an issue regarding the ownership of the '705 Patent. To address that issue, I include a January 8, 2020 assignment from Securicom (NSW) Pty Ltd. ("Securicom") to CPC Patent Technologies Pty Ltd. ("CPC")[1] Therein, Securicom confirms assignment of the IP Rights set forth in the Schedule to such Assignment to CPC. As you will note, item 19 in the Schedule is the '705 Patent. Thus, no other entity is authorized to negotiate with Apple regarding the '705 Patent (or any other asset listed on the Schedule).

The invention of the '705 Patent is graphically depicted in Figure 2 of that patent:

[1] CPC is a wholly-owned subsidiary of Charter.



As shown in Figure 2, the major components of the claimed invention are transmitter and receiver subsystems, which work in concert to provide access to a "controlled item." A "controlled item" can be "an electronic key circuit in a personal computer" that is to be accessed by the user. '705 Patent, col. 6, lines 17-20. Representative claim 1 of the '705 Patent reads as follows:

> A system for providing secure access to a controlled item, the system comprising:
>
> a memory comprising a database of biometric signatures;
>
> a transmitter sub-system comprising:
>
> a biometric sensor configured to receive a biometric signal;
>
> a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and
>
> a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and
>
> a receiver sub-system comprising:

a receiver sub-system controller configured to:

receive the transmitted secure access signal; and

provide conditional access to the controlled item dependent upon said information;

wherein the transmitter sub-system controller is further configured to:

receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

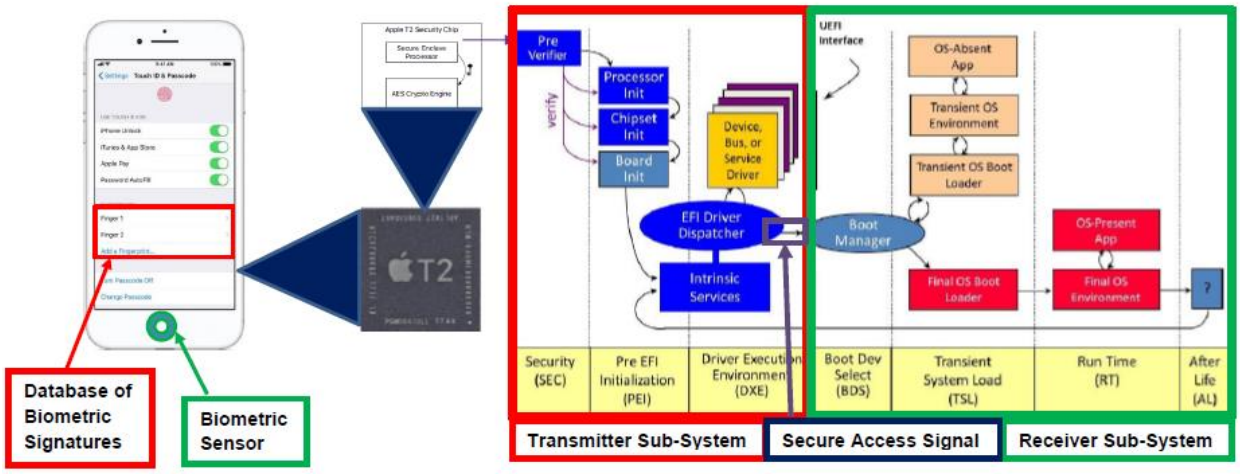
map said series into an instruction; and

populate the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

The "biometric signature" can be a fingerprint (*id.*, col. 7, line 40), and the "biometric sensor" can be a fingerprint sensor (*id.*, col. 5, lines 60-63). Further, the "secure access signal" can be transmitted from the transmitter to the receiver can be over a wired medium. *Id.*, col. 7, lines 9-12. In particular, the controlled item can be an electronic key circuit in a personal computer that is to be accessed by the user. *Id.*, col. 6, lines 17-20. In that case, the computer can store the biometric signature in internal memory, and the computer can be integrated into the receiver sub-system. *Id.*, col. 7, lines 22-26.

On a related note, in your March 5, 2020 letter, you contend that "[t]he intrinsic record of the '705 patent makes clear, however, that the two sub-systems are separate devices that wirelessly transmit signals between them." The afore-quoted passage from the '705 Patent belies that position.

Apple's Touch ID secure access technology, as implemented in, *e.g.*, Apple's iPhone, is described in various Apple publications, such as *Apple T2 Security Chip Security Overview* (Oct. 2018) and *iOS Security* (Sept. 2014). Further, the Apple T2 security Chip implementing such access technology is the subject of third party analyses, such as Davidov, M., *et al., Inside the Apple T2*. Finally, the subject technology is described in Apple patent documents, such as U.S. Patent Appl. No. 2014/0089682. Such information evidences the operation of Apple's Touch ID technology in the manner depicted below:

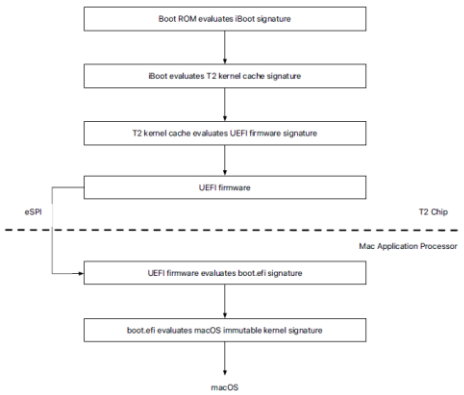


While the above figure illustrates Touch ID as implemented in the iPhone, such illustration is also applicable to Apple's MacBook products:

https://support.apple.com/en-us/HT207054.

The following claim chart demonstrates how claim 10 of the '705 Patent literally reads on Apple's Touch ID devices:

Claim 1	Infringement
A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the	As shown in the figure above, the Apple T2 Security Chip comprises a transmitter sub-system that provides access to the operating system of an Apple device. Also as shown in that figure, access is provided

transmitter sub-system comprises:	to the device's operating system conditioned upon successful completion of the security protocol in the T2 chip.
a biometric sensor configured to receiving [*sic*] a biometric signal;	The Home Button on the iPhone receives fingerprint data to enroll a fingerprint. https://support.apple.com/en-us/HT201371#setup. The Touch ID button on the MacBook receives fingerprint data to enroll a fingerprint. https://support.apple.com/en-us/HT207054.
a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	Secure Enclave is a coprocessor of Apple's T2 Security Chip. *Apple T2 Security Chip Security Overview* (Oct. 2018) at 3. Apple's Secure Enclave is a separate processor built into the device's main system. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/.
a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute	As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green). In the figure below, the transmission is from the T2 Chip to the Mac Application Processor via the Enhanced Serial Peripheral Interface ("eSPI") bus:  *Apple T2 Security Chip Security Overview* (Oct. 2018) at 8.
wherein the controller is further configured to:	The T2 Secure Enclave coprocessor is configured to:
receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&hsimp=yhs-pty_converter&hspart=pty&p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&vid=

	156de65ae06ca453643009fc0ea9cf79&action=click. The user's finger must remain on the home button long enough for the data to be recorded.
map said series into an instruction; and	Registered fingerprint data is stored as mathematical representations. https://support.apple.com/en-us/HT204587. The values are mapped into instructions allowing for a comparison with fingerprints read when unlocking the device. *Id.*
populate the database according to the instruction,	An Apple Touch ID device contains a database with up to five registered fingerprints. https://support.apple.com/en-us/HT201371.
wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	The controlled item is the locked operating system of the Apple device.

While the foregoing analysis is directed to fingerprint data, as claim 4 of the '705 Patent makes clear, the biometric sensor can also be responsive to "face patterns." Thus, the foregoing analysis is also applicable to Apple's facial recognition technology used to unlock more recent models of Apple's devices.

The '705 Patent is only one of the assets owner by Charter for which Apple requires a license. Another such asset is U.S. Patent No. 8,620,039 ("the '039 Patent"), which is attached hereto. The '039 Patent issued on December 31, 2013 from an application claiming priority to an Australian application filed on August 12, 2005. As a result of a patent term extension of 1,707 days, the '039 Patent expires on April 15, 2031. The invention of the '039 Patent is directed to "security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents." '039 Patent, col. 1, lines 14-17. The term "card," as used in the '039 Patent, is synonymous with "card device," and refers to a device containing "card information." *Id.,* col. 1, lines 21-24. The term "reader" includes a receiver that receives card data from the card device. *Id.*, col. 1, lines 55-58.

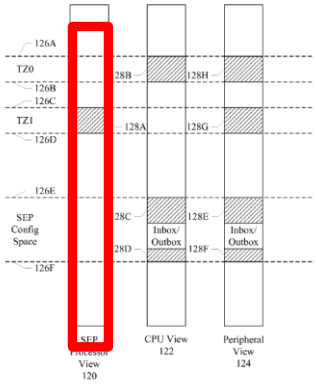
Claim 13 (originally claim 11) received a first office action allowance from the United States Patent and Trademark Office. Office Action (Feb. 26, 2013) at 3. The reason for allowance was that "[n]one of the prior art teaches or suggests defining a memory location in a local memory external to a card in dependence on information received from the card and when that memory is deemed to be unoccupied, storing a received biometric signature therein." *Id.*

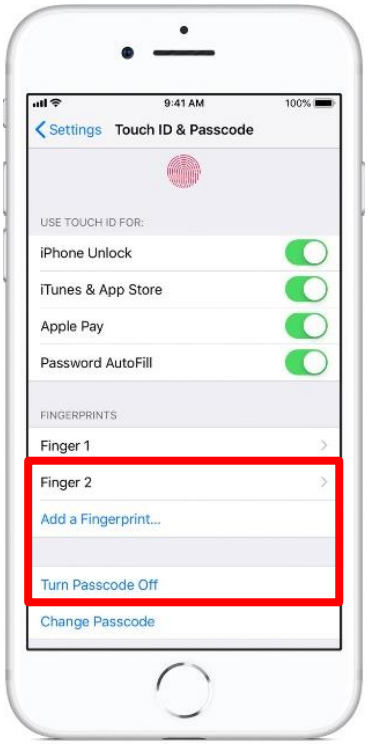
There are two main components to the subject technology - Touch ID (discussed above), and the Apple Card, which is a Sachs-linked credit card. https://www.cnbc.com/2019/03/25/apple-unveils-new-credit-card-the-apple-card.html. The Apple Card is available through the Apple Wallet app on iPhone and makes use of Apple Pay. https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/.

The following chart shows how claim 13 of the '039 Patent reads on the Apple Card used in conjunction with Touch ID biometric security:

'039 Patent	Apple Card
13. A biometric card pointer enrolment system comprising:	Apple's CPU processor encryption includes a pointer to a memory location at which the data to be encrypted is stored. U.S. Patent Appl. No. 2014/0089682 ("the '682 Application"), ¶ [0083]. Apple Card is a Sachs-linked credit card. https://www.cnbc.com/2019/03/25/apple-unveils-new-credit-card-the-apple-card.html.
a card device reader for receiving card information;	Apple's Secure Enclave is a separate, isolated processor built into the device's main system-on-a-chip with a separate processor and area of memory. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/. "Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave." https://support.apple.com/en-us/HT204587. Utilizing Touch ID, the Apple Card uses a "unique security and privacy architecture," *i.e.*, the Secure Enclave receives information from the Apple Card to pair with stored fingerprint data. https://www.creditcardinsider.com/credit-cards/goldman-sachs/apple-card/.
a biometric reader for receiving the biometric signature;	The Home Button on the Apple iPhone receives fingerprint data to enroll a fingerprint. https://support.apple.com/en-us/HT201371#setup.
means[2] for defining, dependent upon the received card information, a memory location in a local memory external to the card;	Apple's Secure Enclave is a separate, isolated processor built into the device's main system-on-a-chip with a separate processor and area of memory. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/. Apple Card is built into the Apple Wallet app on iPhone, *i.e.*, the Secure Enclave memory is external to the Apple Card. *See* https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/.

[2] The "means" described in the '039 Patent specification for performing the claimed function is computer code. '039 Patent, col. 2, lines 18-19, col. 4, lines 62-67 & col. 5, lines 21-23.

	The address locations of an Apple security enclave are depicted below:  '682 Application, ¶ [0018] & Fig. 7.
means for determining if the defined memory location is unoccupied; and	Up to five fingerprints can be registered for Apple Touch ID. https://support.apple.com/en-us/HT201371. Deleting a stored fingerprint requires user action, i.e., stored fingerprints are not over-written by new fingerprints once the five fingerprint maximum has ben reached. *Id*. The foregoing evidences that each registered fingerprint is stored in a separate memory location that must be empty to accommodate such storage, which requires determining that a memory address is unoccupied.
means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.	"Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave." https://support.apple.com/en-us/HT204587. New fingerprint data is enrolled via Touch ID for comparison against fingerprint data subsequently acquired by the Touch ID sensor. iOS Security (Sept. 2014) at 7. Each stored fingerprint is identified to a user in a list presented in the interface, evidencing fingerprint storage:

Again, while the foregoing is directed to a fingerprint as the biometric signature, the '039 Patent teaches that the biometric signature can be a "face." '039 Patent, col. 7, lines 45-47. Thus, to the extent Apple incorporates facial recognition as the mechanism for accessing the Apple Card, such access would be covered by claim 13 of the '039 Patent as well.

I have attached hereto a list of patent assets owned by Charter and available for licensing. I would appreciate the chance to discuss this matter with you further, and propose a telephone conference on April 1, 2020 at 10:00 your time. If there is another date and time that would be more convenient for you, please let me know. If you refer this matter to another individual, please provide me the contact information for that individual.

Very truly yours,

/s/ George C. Summerfield
George C. Summerfield

cc: Kevin Dart (w/out attachments)

Attachments